review ITFORUM 2020 / ВЗГЛЯД В БУДУЩЕЕ

Слабое звено

По прогнозу аналитиков, рынок решений в области мобильной безопасности уже через пару лет вырастет почти на 300%. Офисные сотрудники все чаще предпочитают использовать на работе личные мобильные устройства, и этот факт требует пересмотра подходов в организации корпоративных систем информационной безопасности.

Самая большая угроза корпоративной безопасности в 2013 году останется неизменной: конечный пользователь. Это всегда будет слабым местом

ФОТО ОЛЕГА ХАРСЕЕВА

Угроза обнаружена

Рынок решений в области мобильной безопасности, по прогнозам компании IDC, к 2016 году вырастет на 298% и составит $1,77 млрд. И это понятно: одними из самых сильных тенденций, несущих риски безопасности корпоративным информационным системам, являются консьюмеризация и политика Bring Your Own Device. Сотрудники компаний все чаще хотят использовать сервисы, устройства и ПО то же самое, что и за пределами офиса. Причем задействовать в своей работе офисные служащие предпочитают свои личные устройства, а не корпоративные. Согласно февральскому исследованию Forrester, проведенному по заказу компании TrendMicro, 78% руководителей высшего звена в Европе и США уже столкнулись с тем, что их сотрудники используют свои личные устройства для работы. В России такая практика еще не настолько распространена, но уже создает серьезные проблемы специалистам по корпоративной безопасности. Компания «Астерос» говорит о 30-процентном проникновении этого тренда в отечественный бизнес.

Все это происходит на фоне постоянно растущей активности киберпреступности. В третьем квартале текущего года, по данным «Лаборатории Касперского», в рейтинге стран по количеству вредоносных хостингов Россия потеснила лидера (США): в нашей стране располагается 23,3% «мировых запасов», что на 3% больше показателя Штатов. Правда, есть и хорошие новости: Россия наконец-то перестала возглавлять список самых опасных для вебсерфинга стран мира. Это место занял Таджикистан, где 61,1% пользователей сталкиваются со срабатыванием антивируса при работе в интернете.

Мобильность дает многочисленные преимущества для бизнеса, но вместе с тем ведет и к повышению рисков. Как и прогнозировала компания TrendMicro, этот год ознаменовался постоянным увеличением числа зловредных программ под мобильные платформы. Только во втором квартале «Лабораторией Касперского» было обнаружено 14,9 тыс. вредоносных программ по Android — почти в три раза больше, чем кварталом ранее. Кража мобильных устройств также один из самых популярных способов получить доступ к корпоративным ресурсам компаний. Этот метод используется в 35% всех атак, если верить данным исследований Ponemon Institute за 2011 год.

Крепкий фундамент

Как защитить корпоративные информационные системы от всех этих угроз? Региональный директор TrendMicro в России и СНГ Вениамин Левцов рассказывает, что и сегодня, и в будущем классический набор инструментов ИБ будет по-прежнему необходим. Его основные составляющие — система политик ИБ предприятия и регулярных аудитов состояния информационной безопасности, мощный аппаратный корпоративный firewall, антивирусы на конечных станциях, почте и вебшлюзах, система корпоративного антиспама, механизмы внутрисетевой безопасности, служащие для предотвращения сетевых атак. «Рост интереса к «облачным» технологиям и виртуализации вызывает быстрые изменения ландшафта IT-инфраструктуры, и, как следствие, меняется спектр IT-угроз»,— добавляет господин Левцов. Эта область, безусловно, продолжит развиваться. Глава представительства VMware в России и СНГ Александр Василенко уверен, что компаниям нужно менять архитектуру и подходы к корпоративной инфраструктуре. «Требования, которые идут от бизнеса,— получать больше при меньших ресурсах и затратах — невозможно реализовать на старой платформе, именно поэтому виртуализация и «облака» сейчас так востребованы»,— говорит господин Василенко.

По мнению Вениамина Левцова, повестка завтрашнего дня на рынке систем корпоративной безопасности будет сосредоточена вокруг следующих трендов. В связи с проникновением «облачных» технологий и механизмов становится актуальным перенос акцентов защиты с конечных точек на серверные емкости. Объем данных растет, значит, гораздо эффективнее производить обновления и вычисления централизованно, а конечные точки использовать в рамках идеологии терминального доступа. Технически защита серверов сейчас фактически означает интеграцию средств ИБ с интерфейсом платформы виртуализации.

Второй тренд — использование автоматизированных систем патч-менеджмента. «На сегодняшний день еще далеко не все компании выстроили надежную систему обнаружения уязвимостей и автоматизированного патчинга (установке обновлений. — «Ъ»)», — заключает господин Левцов. Также все более активно используются Web Application Firewall — межсетевые экраны, контролирующие поведение конкретных приложений. А рост таргетированных атак (APT), особенно на крупные организации, требует внедрения соответствующих решений.

Закомплексованная защита

Представители компании КРОК подтверждают, что интерес заказчиков к теме информационной безопасности в России растет. Одна из причин — требования регуляторов относительно соблюдения закона N152-ФЗ «О персональных данных». Кроме того, повышенное внимание к защите необходимо в свете распространения «облаков» и виртуализации, дистанционного банковского обслуживания и т. д.

Михаил Башлыков, руководитель направления информационной безопасности компании КРОК, рассказывает, что сегодня на рынке существуют решения, актуальные практически для всех крупных компаний, например DLP-системы для защиты от утечки конфиденциальной информации. Также с распространением мобильных технологий все большую популярность приобретают соответствующие решения: помимо ограничений доступа к устройству с помощью паролей и шифрования хранящейся там информации распространяются MDM-системы для централизованного управления параметрами безопасности, виртуальные защищенные пространства для удаленного взаимодействия с корпоративными системами и т. д.

«Общий тренд в сфере безопасности — комплексный подход, — утверждает Михаил Башлыков. — Сейчас большинство проектов мы начинаем с аудита, находим уязвимые места в информационных системах и интегрируем средства защиты с существующими бизнес-приложениями так, чтобы эффект был максимален без существенных изменений в работе пользователей».

Алексей Ивлев, руководитель практики консалтинга в области информационной безопасности Accenture, полагает, что для создания полноценной защиты необходимо применять комплексный подход, основанный на нескольких составляющих: стратегический уровень, защита мобильных устройств, сетевая защита, защита мобильных приложений, защита back-end систем. На стратегическом уровне должна быть разработана стратегия, которая определяет критичные направления посредством анализа рисков и позволяет четко спланировать действия по защите мобильных устройств и технологий.

По словам господина Ивлева, защита мобильных устройств обязана включать целый комплекс мероприятий по обеспечению безопасности девайсов и данных, хранящихся на них. Должна быть предусмотрена возможность удаленного блокирования устройств, сброса к заводским установкам или выборочного удаления информации на них, выполнения резервного копирования конфигурации, данных и приложений на мобильных устройствах, использования средств централизованного обновления ОС и ПО на мобильных устройствах и т. п. На уровне сетевой защиты господин Ивлев рекомендует не забывать про VPN-каналы, а также защиту периметра корпоративной сети компании посредством межсетевых экранов и средств IDS/IPS.

Защита мобильных приложений должна включать создание каталога корпоративных программ, черных и белых списков для ограничения использования несанкционированного ПО, анализ безопасности кода при разработке собственных корпоративных мобильных приложений. «Также необходимо помнить о защите самих back-end систем, к которым осуществляется доступ с мобильных устройств,— добавляет Алексей Ивлев.— Однако это скорее теоретическая модель безопасности, на практике по нашему опыту, как правило, все значительно проще: компании ограничиваются только базовым набором мер защиты, поскольку выполнение полного спектра мероприятий довольно затратно и не всегда оправданно имеющимися рисками ИБ. Особенно это актуально для российских компаний, которые только начинают внедрять мобильные технологии в корпоративную среду».

Выйти из сумерек

У российских компаний сильно разнится отношение к желанию сотрудников использовать личные устройства и привычные сервисы на работе. Сергей Орлик, директор центра корпоративной мобильности «АйТи», говорит, что «наиболее простая, рефлекторная реакция, часто наблюдаемая в крупных организациях, проявляется в первоначальном решении «запретить»». Но при этом доступ к корпоративной информации с мобильных устройств — реальная потребность руководителей всех уровней и сотрудников, стремящихся повысить продуктивность своей деятельности.

Господин Орлик рассказывает, что ИБ-решения, которые необходимы в связи с этим частным компаниям, требуют инвестиций, причем существенно отличающихся от стоимости приложений или игр в AppStore. «Но только полноценная инфраструктура корпоративной мобильности может превратить смартфоны и планшеты в удобные для пользователя и безопасные для организации мобильные рабочие места, необходимость в которых пользователи уже подтвердили массовым использованием современных гаджетов,— убежден он.— По сути, системность подхода в организации мобильных рабочих мест заключается в том, что в отношении практически всего ИБ-ландшафта организации необходимо добавить новый срез, или, если хотите, новое измерение, связанное с мобильными рабочими местами. Если этого не сделать, оставшись в традиционном контексте формального запрета, возникают «теневые IT», с которыми связаны и несоизмеримо более высокие риски, и непосредственные затраты на последующий «вывод из тени»».

Валерий Андреев, заместитель директора по науке и развитию компании ИВК, убеждает в том, что сегодня руководители компаний уже понимают, что многие нововведения, как аутсорсинг или BYOD, действительно полезны предприятию. Поэтому запрещать становится все труднее и приходится проблему решать. Но не имея типовых практик, необходимо искать и находить свои пути решения новых старых проблем и научиться их защищать на основе имеющихся методик построения моделей угроз, создания полных и непротиворечивых систем защиты и пр. «При этом компании должны учесть, что между подходами к созданию систем ИБ сегодня и вчера существует огромная разница. В прежние годы функциональность информационной системы всегда ставилась во главу угла, а системы ИБ докручивались (или даже и не докручивались) потом. Это и раньше создавало практически неразрешимые проблемы информационной безопасности. Но нынешние вызовы ИБ изначально столь опасны, что без применения интегрированных средств защиты уже сама функциональность ИС ставится под сомнение», говорит господин Андреев.

Гэри Кларк, вице-президент компании SafeNet в регионе EMEA, добавляет: «В конечном счете, самая большая угроза в 2013 году останется неизменной: конечный пользователь. Это всегда будет слабым местом. Причина проста. Многие компании все еще полагаются на ненадежные пароли для защиты доступа к данным, и до сих пор атаки на пароли были самым простым путем получения доступа к системе и приложениям, особенно когда компании все еще не шифруют свои данные для необходимой степени защиты». По мнению господина Кларка, все компании должны сделать два основных шага: избавиться от паролей и заменить их на одноразовые, а также зашифровать все конфиденциальные данные. Эту точку зрения поддерживает Катажина Хоффманн, региональный менеджер по продажам решений логического доступа компании HID Global в Восточной Европе: «Для того чтобы доверять корпоративным пользователям и эффективно управлять их доступом к информационным ресурсам, компаниям необходимо комплексное решение, обеспечивающее идентификацию».

Антон Разумов, руководитель группы консультантов по безопасности компании Check Point Software Technologies, добавляет: «Кто всерьез воспринимал социальные сети как опасность пять-семь лет назад? А сейчас для всех очевидно, что пользователи, в том числе крупные руководители, бездумно размещают в интернете весьма конфиденциальные документы, информацию о клиентах, планах компании». При этом блокирование подобных ресурсов не даст эффекта: сотрудники научились для этого пользоваться личными устройствами. Господин Разумов считает, что гораздо эффективнее контролировать пользователей, обучать их, предупреждать, когда они делают что-то неправильное.

К сожалению, на данный момент значительное количество IT-специалистов не обладает достаточными знаниями о современных киберугрозах. Кроме того, низкий уровень компьютерной грамотности персонала является одной из причин заражения IT-инфраструктуры компании и утечки конфиденциальной информации. Поэтому обучение всех сотрудников компании основам информационной безопасности не менее важно, чем установка современного защитного ПО.

Светлана Рагимова

АКТУАЛЬНО

Talk show: «Будущее информационной безопасности промышленных объектов и инфраструктур в России». 17 апреля 2013. 13.30–15.30. Ярмарочный комплекс, павильон №1, центральная сцена.

Как правило, для критически важных объектов существуют достаточно жесткие требования к безопасности. Но выполнение этих требований в каждой из критических точек зачастую бывает не просто, не бесплатно, связано с дополнительными расходами времени и усилий, а потому случается, что такого рода требования просто не выполняются. Те же, кому поручено отвечать за безопасность на том или ином участке, зачастую опасаются докладывать руководству о реальном положении, опасаясь обвинений в том, что они не справляются со своими обязанностями. Нередко в организациях царит атмосфера «святой лжи», когда все знают, что важные требования для многих уязвимых мест не выполняются, но везде рапортуется о полной безопасности. Главный порок такой ситуации состоит в том, что руководство, в руках которого находится доступ к ресурсам, с помощью которых проблемы с безопасностью во многих случаях могли бы быть решены, не знает истинного положения дел. Вместе с тем нельзя не признать, что порой побудителями культивирования «святой лжи» являются «веские» причины, а именно понимание того, что если выполнять все требования по безопасности, то организация, может, и не выдержит этого, утратив свою экономическую конкурентоспособность.

Что смотреть

VI Международный форум «ITForum 2020/ Взгляд в будущее» предлагает участникам посетить более 50 разнонаправленных мероприятий: государственное управление, здравоохранение, образование, промышленность, бизнес и досуг. Круглые столы и мастер-классы открыты для людей разных возрастных категорий и сфер деятельности. Ъ-Review «IT-Forum» предлагает обзор наиболее интересных мероприятий.

В рамках road show Russian Startup Tour представители российских институтов развития проведут несколько открытых мастер-классов по созданию, финансированию и продвижению стартапов, а успешные региональные стартаперы поделятся с нижегородскими предпринимателями своим опытом. Кроме того, региональных бизнесменов ждет закрытый бизнес-тренинг (коучинг) от представителей фонда «Сколково». Отметим, что «Сколково» проведет еще одно мероприятие на форуме — конференцию кластера информационных технологий фонда.

Несколько крупных мероприятий форума в этом году посвящено информационным технологиям в сфере госуправления. Организаторы предлагают проанализировать и обсудить перспективы развития портала госуслуг: от видов и количества услуг, переведенных в электронный вид, до психологических проблем и барьеров у представителей органов исполнительной власти и местного самоуправления, вызванных этим переводом. Несколько часов участники форума посвятят обсуждению инновационных решений для правительств регионов. Эксперты познакомят участников с концепцией электронного управления основными процессами жизнедеятельности городов — «Разумный город», поговорят об условиях успешного внедрения интеллектуального операционного центра и об управлении социальными программами. В отдельный блок организаторы вынесли обсуждение развития информационных технологий в здравоохранении, например итоги и перспективы внедрения IT в рамках региональной программы модернизации здравоохранения Нижегородской области.

Министр информационных технологий, связи и СМИ Нижегородской области Сергей Кучин сообщил, что отправится на мастер-класс компании Intel по обучению пенсионеров компьютерной грамотности в рамках национальной программы «Бабушка и дедушка онлайн». «Также я буду участвовать в обсуждении цифрового телевидения и не смогу исключить из своей программы мероприятия, связанные с госуслугами, — ту же комиссию Совфеда. Потому что СМЭВ сегодня — тема для нас и больная, и прорывная, и очень заметная для населения. Ее невозможно игнорировать», — пояснил министр.

16 АПРЕЛЯ / ЯРМАРОЧНЫЙ КОМПЛЕКС, ПАВИЛЬОН № 1

VIP-обход экспозиции 09.30–10.30

Хакатон INTEL 10.30–14.30

Открытый урок INTEL 15.00–16.00 и 16.30–17.30

по обучению компьютерной грамотности в рамках национальной программы «Бабушка и дедушка онлайн»

16 АПРЕЛЯ / ГЛАВНЫЙ ЯРМАРОЧНЫЙ ДОМ. ГЕРБОВЫЙ ЗАЛ

Блок мероприятий Russian Startup Tour 09.30–13.45

«Быть предпринимателем тяжело, но не опасно» (Пекка Вильякайнен). Сервисы для стартапов: продвижение, образование, финансирование, выступление представителей региональных стартап-проектов

16 АПРЕЛЯ / ГЛАВНЫЙ ЯРМАРОЧНЫЙ ДОМ. АКАДЕМИЧЕСКИЙ ЗАЛ

Расширенное заседание 10.30–12.30

временной комиссии Совета федерации по развитию информационного общества

Дискуссионная панель 13.30–18.30

с участием Министерства связи и массовых коммуникаций РФ «Обсуждение региональной информатизации»

16 АПРЕЛЯ / ГЛАВНЫЙ ЯРМАРОЧНЫЙ ДОМ. УНИВЕРСИТЕТСКИЙ ЗАЛ

Круглый стол 10.30–13.00

«Повышение компьютерной грамотности населения»

Региональная конференция 14.00–16.30

«Развитие информационных технологий в российском здравоохранении»

16 АПРЕЛЯ / ГЛАВНЫЙ ЯРМАРОЧНЫЙ ДОМ. ЗАЛ БЕТАНКУРА

Круглый стол 10.00–13.00

«Инновационные решения для правительства региона»

Круглый стол 14.00–16.30

«Big Data: Большие возможности»

Круглый стол 16.30–18.00

«Развитие территорий»

16 АПРЕЛЯ / ЯРМАРОЧНЫЙ КОМПЛЕКС, ПАВИЛЬОН № 1, ЦЕНТРАЛЬНАЯ СЦЕНА

Дискуссионный клуб 10.30–12.30

«Social Media и СМИ: слияние или поглощение?»

Форсайт 14.00–16.00

Молодежного инновационного центра по направлению «Информационные технологии и телекоммуникации»

Ток-шоу 17.00–18.00

«Каким будет обучение компьютерной грамотности будущего»

16 АПРЕЛЯ / ГЛАВНЫЙ ЯРМАРОЧНЫЙ ДОМ. ПРЕЗИДЕНТСКИЙ ЗАЛ

Круглый стол 13.00–16.00

в рамках Skolkovo Startup Tour «Коммерциализация научных разработок: путь к успеху»

16 АПРЕЛЯ / ЯРМАРОЧНЫЙ КОМПЛЕКС, ПАВИЛЬОН № 3

Стратегическая сессия 12.45–15.00

«Инициативы создания регионального предпринимательского сообщества» (АСИ) в рамках Russian Startup Tour

Коучинг 12.45–15.00

региональных стартапов (закрытый формат) представителями фонда «Сколково» в рамках Russian Startup Tour

Презентации 15.15–16.00

по результатам бизнес-игры, презентация региональных стартап-проектов, прошедших коучинг. Торжественное закрытие Russian Startup Tour

17 АПРЕЛЯ / ЯРМАРОЧНЫЙ КОМПЛЕКС, ПАВИЛЬОН № 1, ЦЕНТРАЛЬНАЯ СЦЕНА

Дискуссионный клуб 09.30–10.30

«Social Media для бизнеса: тренды»

Дискуссионный клуб 13.30–15.30

«Будущее информационной безопасности промышленных объектов и инфраструктур в России»

Демонстрация творческих проектов 15.30–16.30

отборочных состязаний Международной робототехнической олимпиады для школьников и студентов “Программирование Лего-роботов” (АНОО НИИТ)

17 АПРЕЛЯ / ЯРМАРОЧНЫЙ КОМПЛЕКС, ПАВИЛЬОН № 1

Открытый урок INTEL 09.30–17.00

по обучению компьютерной грамотности в рамках национальной программы «Бабушка и дедушка онлайн»

17 АПРЕЛЯ / ГЛАВНЫЙ ЯРМАРОЧНЫЙ ДОМ. АКАДЕМИЧЕСКИЙ ЗАЛ

Заседание клуба IT-директоров 09.30–12.30

«Современные тренды в IT и обеспечение их безопасности»

Круглый стол 14.00–18.00

«Свободное программное обеспечение в России: кейсы, прогнозы, футуристика»

17 АПРЕЛЯ / ГЛАВНЫЙ ЯРМАРОЧНЫЙ ДОМ. УНИВЕРСИТЕТСКИЙ ЗАЛ

Круглый стол 09.15–13.00

«Создание многофункциональных центров предоставления государственных и муниципальных услуг в регионах России»

Круглый стол 14.00–16.00

«Актуальные вопросы внедрения универсальной карты в РФ»

17 АПРЕЛЯ / ГЛАВНЫЙ ЯРМАРОЧНЫЙ ДОМ. ЗАЛ БЕТАНКУРА

Дискуссионная панель 09.00–10.30

«Переход к облачным технологиям»

17 АПРЕЛЯ / ГЛАВНЫЙ ЯРМАРОЧНЫЙ ДОМ. КОМНАТА ПЕРЕГОВОРОВ

Круглый стол 11.00–13.00

«Цифровое вещание: перспективы развития телевидения в регионах»

Круглый стол 14.00–17.30

«Информационно-коммуникационные технологии в образовании»

18 АПРЕЛЯ / ЯРМАРОЧНЫЙ КОМПЛЕКС, ПАВИЛЬОН № 1

Открытый урок INTEL 10.00–17.00

по обучению компьютерной грамотности в рамках национальной программы «Бабушка и дедушка онлайн»

Более подробную программу мероприятий, а также точное время вы можете найти на сайте форума http://itforum2020.ru/